REMARKS

No claims have been amended, and no claims have been cancelled. Claims 1-44 therefore remain pending in the application. Applicant respectfully traverses the Office's rejections and, in view of the following remarks, respectfully requests that the Office issue a Notice of Allowance.

§ 102 REJECTIONS

Claims 1, 2, 3, 5, 7, 8-10, 18-19, 21-23, 31-33, and 35-37 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,446,205 (Lenstra). Applicant respectfully traverses the rejections for at least the reasons discussed below, as well as for the reasons discussed during the afore-mentioned interview.

THE CLAIMS

Claim 1 recites a method for use in curve-based cryptography comprising:

- determining a curve for use in cryptographically processing information;
- determining pairings for cryptographically processing said information using a parabola associated with said curve; and
- encrypting the selected information based on the pairings.

In making out a rejection of this claim, the Office alleges that Lenstra anticipates. Office Action mailed 1/11/2008, p. 2. Applicant respectfully disagrees, and instead submits that Lenstra at least fails to disclose or suggest "determining pairings for cryptographically processing said information *using a parabola* associated with said curve" as recited in claim 1 (emphasis added).

Instead, Applicant respectfully submits that Lenstra is directed to selecting an elliptic curve from a set of known elliptic curves, as opposed to using a single elliptic curve for all key generation. Lenstra, abstract, col. 2 lines 1-10. Through these means, Lenstra attempts to increase the number of elliptic curves used by the system, thereby reducing the vulnerability of the crypto-system to attack. Lenstra, Background.

Applicant respectfully submits that Lenstra merely discusses traditional techniques for determining computing pairings. These traditional techniques do not disclose or suggest "determining pairings for cryptographically processing said information *using a parabola* associated with said curve" as recited in claim 1. During the aforementioned interview, the Office agreed that this claim is allowable. Applicant thanks the Office for this indication.

For at least these reasons, claim 1 is allowable.

Claims 2-17 depend from claim 1 and, as such, the remarks made above in regards to claim 1 apply equally to claims 2-17. Claims 2-17 are also allowable for their own recited features, which the references of record have not been shown to disclose, teach, or suggest. Applicant therefore submits that each of claims 2-17 is allowable at least for its dependency upon claim 1.

Claim 18 recites a computer-readable storage medium having computer-implementable instructions for causing at least one processing unit to perform acts comprising:

- determining at least one curve for use in cryptographically processing selected information;

- calculating pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve; and
- cryptographically processing said selected information based on said pairings.

In making out a rejection of this claim, the Office alleges that Lenstra anticipates. Office Action, p. 2. Applicant respectfully disagrees, and instead submits that Lenstra at least fails to disclose or suggest "calculating pairings for use in cryptographically processing said selected information *by selectively using at least one parabola* associated with said at least one curve" as recited in claim 18. During the aforementioned interview, the Office agreed that this claim is allowable. Applicant thanks the Office for this indication.

For at least this reason, claim 18 is allowable.

Claims 19-30 depend from claim 18 and, are allowable by virtue of this dependency. Claims 19-30 are also allowable for their own recited features, which the references of record have not been shown to disclose, teach, or suggest. Applicant therefore submits that each of claims 19-30 is allowable at least for its dependency upon claim 18.

Claim 31 recites an apparatus comprising:

- memory configurable to store information; and
- logic operatively coupled to said memory and configurable to at least support cryptographic processing of selected information stored in said memory by determining at least one curve for use in cryptographically processing selected information and determining pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve.

In making out a rejection of this claim, the Office alleges that Lenstra anticipates. Office Action, p. 2. Applicant respectfully disagrees, and instead submits that Lenstra fails to disclose or suggest "determining pairings for use in cryptographically processing said selected information by selectively *using at least one parabola* associated with said at least one curve" as recited in claim 31. During the aforementioned interview, the Office agreed that this claim is allowable. Applicant thanks the Office for this indication.

For at least this reason, claim 31 is allowable.

Claims 32-44 depend from claim 31 and, are allowable by virtue of this dependency. Claims 32-44 are also allowable for their own recited features, which the references of record have not been shown to disclose, teach, or suggest. Applicant therefore submits that each of claims 32-44 is allowable at least for its dependency upon claim 31.

CONCLUSION

For at least the foregoing reasons, claims 1-44 are in condition for allowance. Applicant respectfully requests reconsideration and withdrawal of the rejections and an early notice of allowance. If any issue remains unresolved that would prevent allowance of this case, Applicant respectfully requests the Office to contact the undersigned representative to resolve the issue.

Lee & Hayes, PLLC
Representatives for Applicant

/David W. Foster/ Dated: 6/10/2008

David W. Foster (daved@leehayes.com)
Reg. No. 60,902
Robert G. Hartman (rob@leehayes.com)
Registration No. 58,970

Customer No. 22801

Telephone: (509) 324-9256
Facsimile: (509) 323-8979
www.leehayes.com